27th ANNUAL

FIRST CONFERENCE BERLIN

14-19 JUNE 2015

UNIFIED SECURITY: IMPROVING THE FUTURE

Seven Years in MWS

Experiences of the community based data sharing for anti-malware research in Japan

Masato TERADA (MWS organization committee / Hitachi Incident Response Team)

Mitsuhiro HATADA (MWS organization committee / NTT Communications Corporation)

Yoichi SHINODA (MWS organization committee / Japan Advanced Institute of Science and Technology)

Opening

7 years ago, in 2008, the anti-Malware engineering WorkShop (MWS) started in Japan. The main objective of MWS is to accelerate and expand the activities of anti-malware research and countermeasure.

This presentation describes MWS, which is academic, enterprise and public domains joint activities in Japan.

ANTI MALWARE ENGINEERING WORKSHOP
MWS

Main objective of MWS

7 years ago, MWS started in 2008.

MWS is organized by MWS community in IPSJ,
Information Processing Society of Japan. 一般社団法人 情報処理学会 Information Processing Society of Japan

Main objective of MWS

Anti-malware researchers and engineers of academic, private (enterprise) and public domains join MWS community to accelerate and expand the activities of anti-malware research.

To this end, MWS aims to attract new researchers, engineers of academic, private (enterprise) and public domains. Also stimulate new research for addressing latest cyber threats.

MWS Activities

MWS has the community based sharing scheme of the datasets for anti-malware research and countermeasure. Also this scheme has three parts to achieve our objective.

MWS Community

The environment to work hard together

MWS Dataset

The datasets sharing for anti-malware research and countermeasure

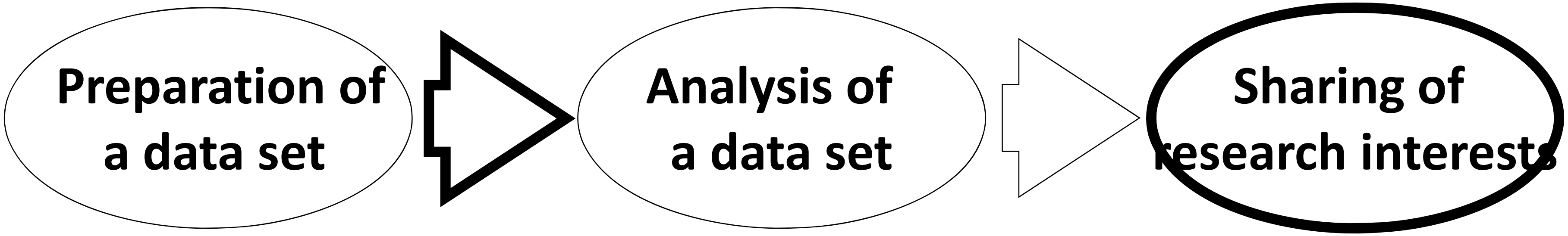
MWS Workshop

The research interests sharing

MWS Activities

Research sections in academic, enterprise and public domains

Academic societies



Preparation of a data set

Analysis of a data set

Sharing of research interests

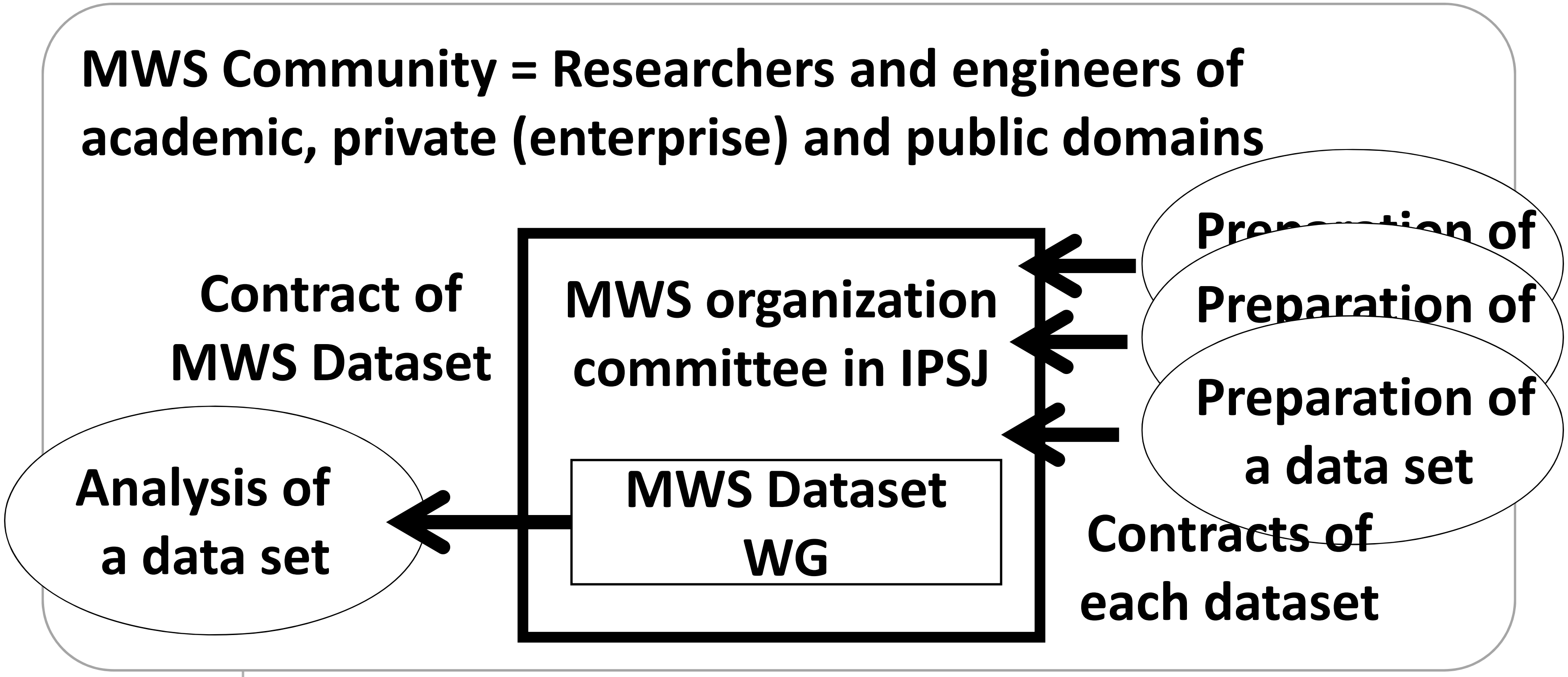
The data set for the research of anti-malware engineering
MWS Dataset

The research interests sharing
MWS Workshop
(=workshop + competition)

The environment to work hard together
MWS community

MWS Community

MWS organization committee in IPSJ is hub function for community based sharing scheme of the datasets.



MWS Community = Researchers and engineers of academic, private (enterprise) and public domains

Contract of MWS Dataset

MWS organization committee in IPSJ

MWS Dataset WG

Analysis of a data set

Preparation of

Preparation of

Preparation of a data set

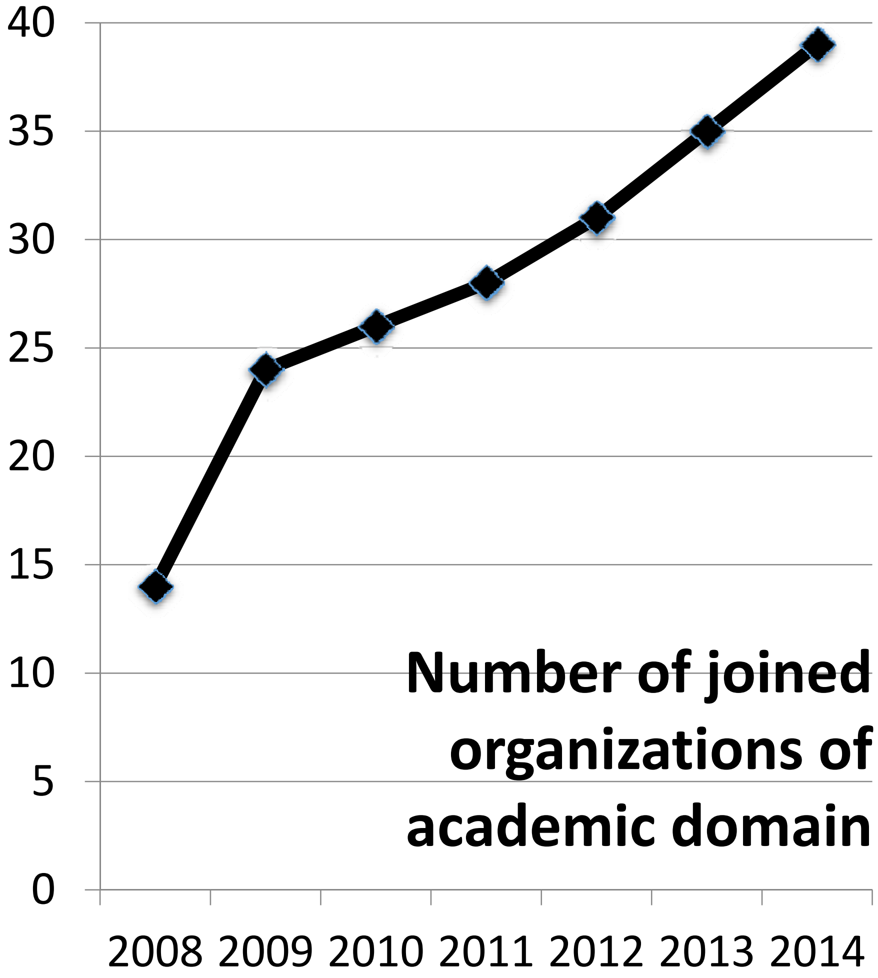
Contracts of each dataset

MWS Community

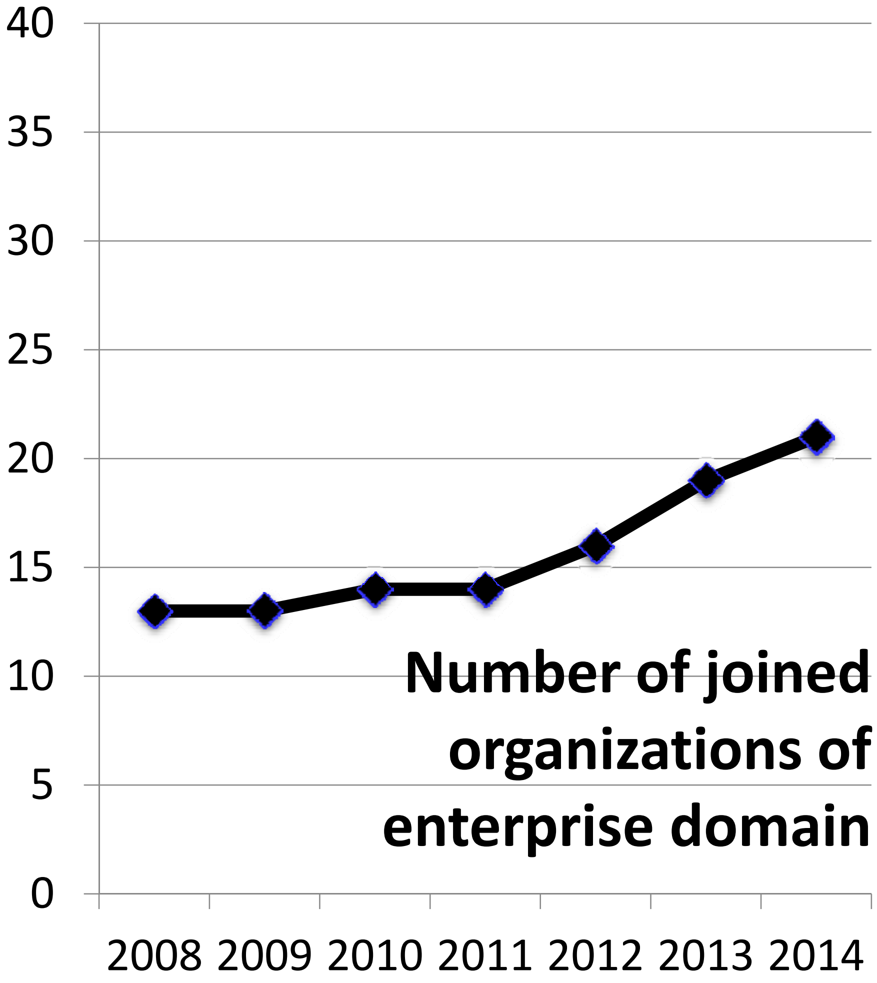
Currently MWS Community has organizations of public domain, academic domain and enterprise domain in Japan. In organizations of public domain, JPCERT/CC, IPA, AIST and NICT joined MWS community.

Also many organizations of academic/enterprise domain joined. Our community scale is larger each year.

MWS Community



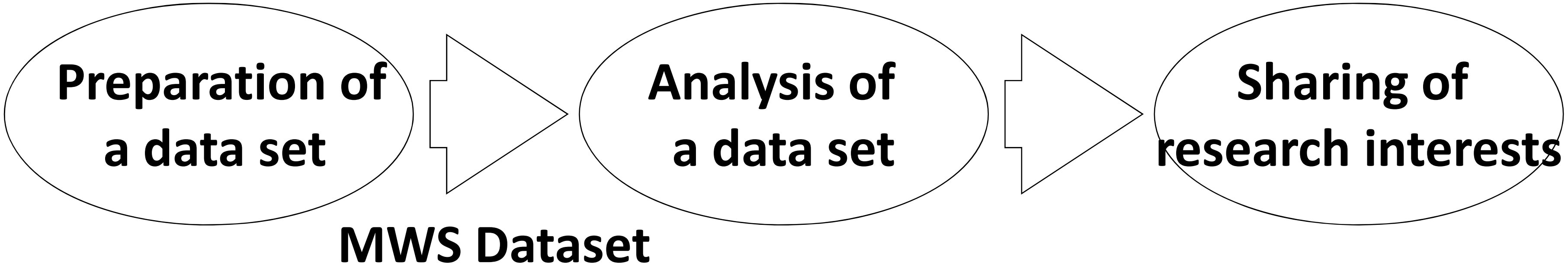
Number of joined organizations of academic domain



Number of joined organizations of enterprise domain

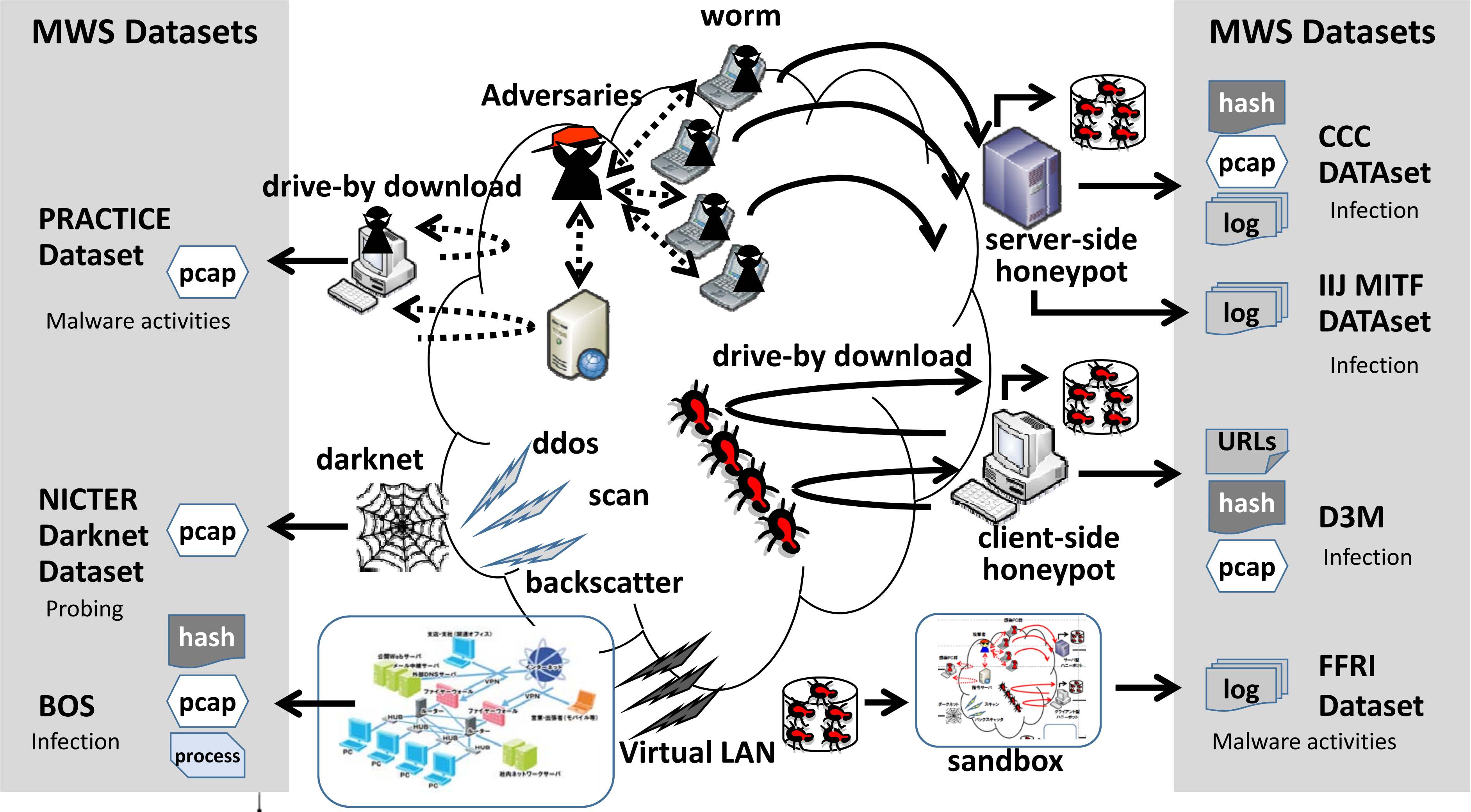
MWS Dataset

Start up phase of the MWS Datasets of framework is "Preparation of a data set".



Start up phase of the MWS Dataset covers three categories, i.e., probing, infection, and malware activities.

MWS Dataset



MWS Datasets

PRACTICE Dataset
pcap
Malware activities

NICTER Darknet Dataset
pcap
Probing

BOS
hash
pcap
process
Infection

worm

Adversaries

drive-by download

darknet

ddos

scan

backscatter

Virtual LAN

sandbox

server-side honeypot

drive-by download

client-side honeypot

MWS Datasets

CCC DATAset
hash
pcap
log
Infection

IIJ MITF DATAset
log
Infection

D3M
URLs
hash
pcap
Infection

FFRI Dataset
log
Malware activities

MWS Dataset

	2008	2009	2010	2011	2012	2013	2014
CCC DATAset [server-side honeypot]	☑	☑	☑	☑	☑	☑	
MARS for MWS [malware dynamic analysis]	☑	☑	☑				
D3M [client-side honeypot]			☑	☑	☑	☑	☑
IIJ MITF DATAset [server-side honeypot]					☑		
PRACTICE Dataset [malware behavior analysis]						☑	
FFRI Dataset [malware sandbox analysis]						☑	☑
NICTER Darknet Dataset [darknet monitoring system]						☑	☑
Behavior Observable System (BOS) [observing threat actors]							☑

MWS Dataset

Start up phase of the MWS Dataset covers three categories, i.e., probing, infection, and malware activities.

Probing

NICTER Darknet Dataset [darknet monitoring system]

MWS Dataset

Start up phase of the MWS Dataset covers three categories, i.e., probing, infection, and malware activities.

Infection

CCC DATAset [server-side honeypot]
IIJ MITF DATAset [server-side honeypot]
D3M [client-side honeypot]

MWS Dataset

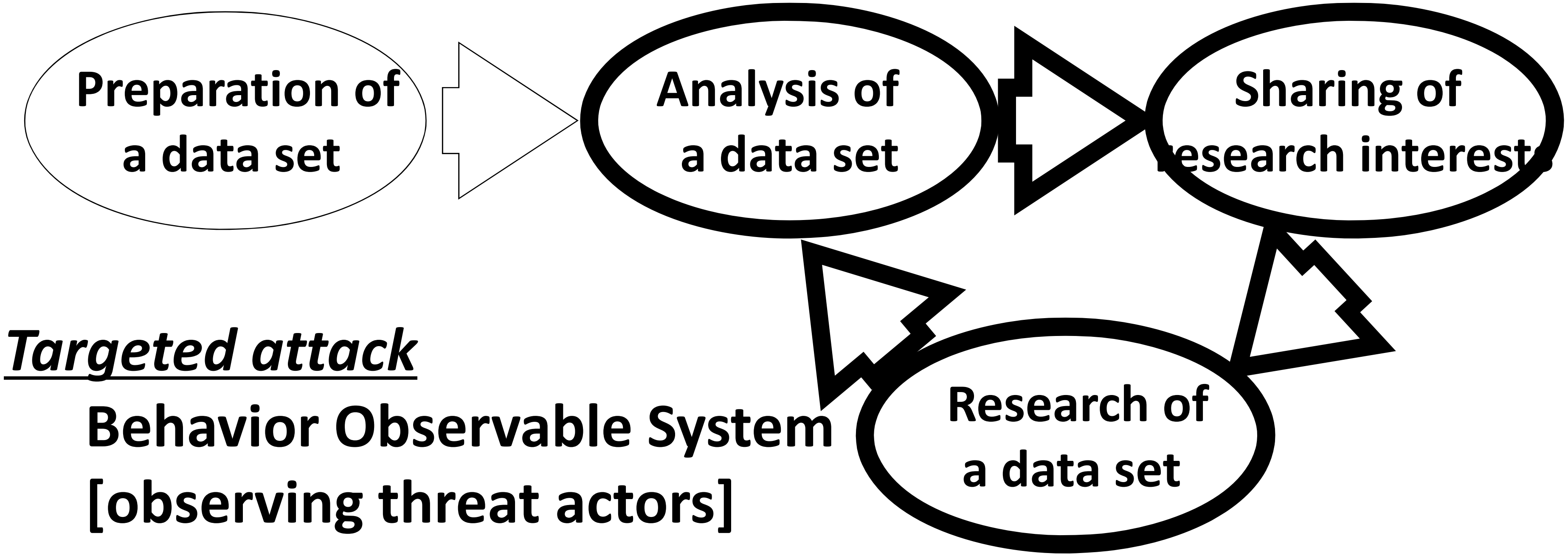
Start up phase of the MWS Dataset covers three categories, i.e., probing, infection, and malware activities.

Malware activities

PRACTICE Dataset [malware behavior analysis]
MARS for MWS [malware dynamic analysis]
FFRI Dataset [malware sandbox analysis]

MWS Dataset

Mature phase of the MWS Dataset of framework is "Research of a data set".



Targeted attack

Behavior Observable System [observing threat actors]

MWS Workshop

MWS Workshop task is to improve an anti-malware research environment such as the detection, the monitoring and the analysis of malware. Also it was to build the collaboration community between the academic field researchers and the enterprise field engineers for the malware countermeasures.

MWS Workshop

MWS includes workshop and competition. Also it has conjunction with CSS (Computer Security Symposium) of the SIG-CSEC, IPSJ.

Oct. 22, 2014	MWS cup (2.5 hr)				
	Drive by download (90min)	Network attack monitoring	Security design and implementation	Risk analysis and policy	Public key
	Evaluation of security technology	Targeted attacks	Security design and implementation	Risk analysis and policy	Public key
Oct. 23, 2014	Network attack monitoring	DDoS	Web security	Malware classification	Evaluation of security technology
	MWS cup presentation	Targeted attacks	Web security	Forensics	Searchable encryption
	Drive by download	Malware static analysis	Web security	Vehicle Security	Secret calculation
	Evaluation of security technology	Targeted attacks	OS/Virtualization	Vulnerability analysis	Proxy re-encryption
Oct. 24, 2014	Malware detection	Malware behavior analysis	Authentication	Privacy	Cryptographic protocol
	Malware detection	Malware behavior analysis	Authentication	Privacy	Cryptographic protocol
	Dataset preparation	Malware behavior analysis	Psychology and trust	Privacy	Cryptographic protocol
	Psychology and trust	Control system security	Information hiding	Privacy	Conference report

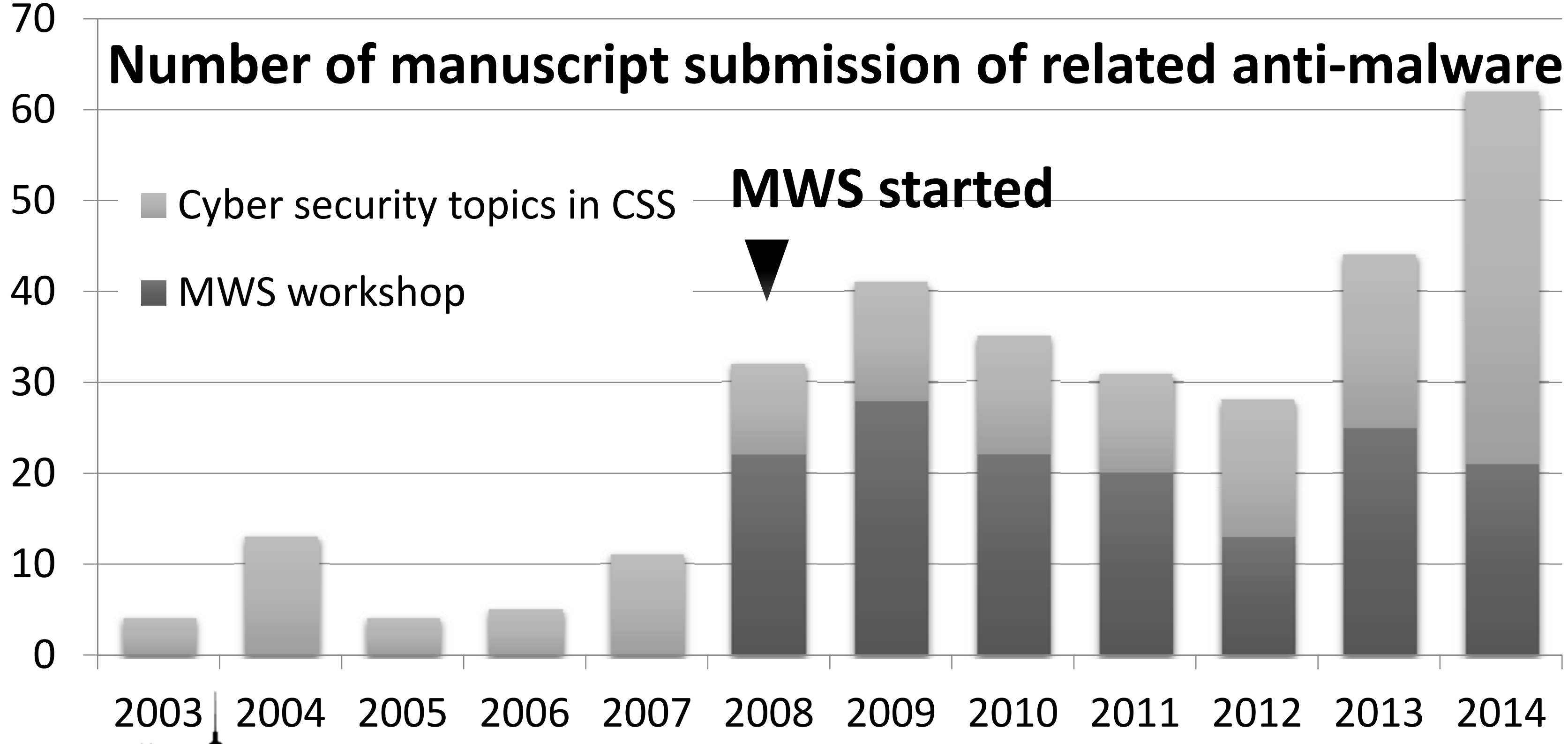
MWS competition

MWS workshop

CSS (Computer Security Symposium)

MWS Workshop

MWS activated the research of related anti-malware domain in Japan.



MWS Workshop

MWS competition (aka. MWS cup) has technical and artistic part.

The MWS organization committee provided the pre-challenges and the challenges of technical part in MWS cup 2014.

MWS Workshop

Timeline

MWS(Oct. 22-24, 2014)

technical part

Sep. 12, 2014

"4 Pre-challenges" published. (22days)

Oct. 3, 2014

Pre-challenges submission deadline.

Oct. 22, 2014 (9:30-12:00)

3 challenges (2.5hr)

Oct. 22, 2014 (12:00)

Challenges submission deadline.

Rules

Joined MWS community: must

Number of team member: no limit

MWS cup 2014

11 teams (about 100 attendees)

artistic part

Oct. 23, 2014 (10:55-12:15)

Very short presentation of resolution approach for pre-challenges and challenges (5min/team)

MWS Workshop

MWS cup 2014 technical part

Pre-challenges

1. Drive-by Download attack PCAP analysis
2. Malware static analysis
3. Malware behavior analysis
4. Darknet packet analysis

Challenges

1. Drive-by Download attack PCAP analysis
2. Malware static analysis
3. Malware behavior analysis

MWS Workshop

ANTI MALWARE ENGINEERING WORKSHOP MWS

MWS cup 2014 technical part

MWS Workshop

Timeline

MWS(Oct. 22-24, 2014)

technical part

Award Winner with Technical Part

70 points

artistic part

Award Winner
with Artistic Part

30 points

Award Winner
Total 100 points

MAC 2014 and MWS

In late October 2014, ThaiCERT, a member of ETDA (Electronic Transactions Development Agency), and JPCERT/CC organized an event "Malware Analysis Competition 2014 (MAC 2014)" in Bangkok, Thailand.

ETDA บ่มเพาะคนพันธุ์ใหม่ รู้ทันภัยมัลแวร์ ด้วยเวทีแข่งขัน MAC 2014

https://www.thaicert.or.th/events/2014/ev2014-11-08-1.html

MAC 2014 and MWS

MAC 2014 in Bangkok, Thailand

ETDA
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
Electronic Transactions Development Agency (Public Organization)
MAC
Fly with
ThaiCERT to APCERT AGM
& Conference 2015, Malaysia
APCERT
ThaiCERT
ETDA

MAC 2014 and MWS

We gave a talk about MWS in Japan. Also the activities of MWS, especially MWS cup was referred to by MAC 2014.

These events are very useful for technical transfer and raising awareness as well as information sharing in the academic, enterprise and public domains for anti-malware research and countermeasure.

Next step of MWS

We believe that our experiences can assist other research communities that have a similar vision and comparable objectives.

Next step of MWS

We are now planning to expand our activities to the global research community in response to several requests for accessing the MWS Dataset from researchers in other countries.

Ending

So we are hoping to continue the effort and also to extend it to more relationships for anti-malware research and countermeasure.

Also we would like to realize joint activities of CSIRT communities as next step.

Collaborate together to make your Internet secure.

Seven Years in MWS

Experiences of the community based data sharing for anti-malware research in Japan

anti Malware engineering WorkShop 2015 (MWS 2015)
http://www.iwsec.org/mws/2015/en.html